

WO 00/14716

PCT/SG98/00067

20

CLAIMS:

1. A method of generating a key or set of keys from a person's biometrics data comprising the steps of:
 - (1) capturing the person's biometric data;
 - (2) normalizing the captured biometrics data,
 - (3) extracting invariant feature measures from the normalized data and representing the feature measures as a bit pattern;
 - (4) storing the bit pattern in associative memory in an enrolment / registration phase and recalling the stored bit pattern from the associative memory in an identification / verification phase; and
 - (5) generating the key from the recalled bit pattern.
2. A method as claimed in Claim 1 wherein the normalization step includes the step of selecting reference points of the captured biometrics data and normalizing the data with respect to the reference points.
3. A method as claimed in Claim 2 wherein the biometrics data comprises a face image and the reference points comprise the location of the eye portions of the face image.
4. A method as claimed in Claim 2 wherein the biometrics data comprises a fingerprint image and the reference points comprise the location and orientation of

00763624.061501

WO 00/14716

PCT/SG98/00067

21

the core of the fingerprint image.

5. A method as claimed in any one of the preceding Claims wherein the biometrics data comprises an image and the features are selected from normalized data corresponding to a portion of the image.

6. A method as claimed in any one of the preceding Claims wherein the bit pattern is generated from the features using a representation scheme.

7. A method as claimed in Claim 6 wherein the features are represented according to importance.

8. A method as claimed in any one of the preceding Claims wherein the image is a fingerprint image and the feature measures are of minutiae points.

9. A method as claimed in any one of Claims 1 to 7 wherein the image is a face image and the feature measures are of corners of the image.

10. A method as claimed in any one of the preceding Claims wherein the associative memory is implemented using a neural network.

11. A method as claimed in claim 10 wherein the neural network is a Hopfield network.

00763624-06160

WO 00/14716

PCT/SG98/00067

22

Sub A3

12. A method as claimed in any one of the preceding claims wherein, in step (5), a symmetry key or public/private key pair is generated.

13. A method as claimed in claim 12 further comprising the step of performing encryption or decryption using the key when inputting or outputting data.

Sub A4

14. A method as claimed in any one of the preceding Claims wherein steps (1)-(4) are applied to a plurality of biometrics data sources, the key being generated from a respective plurality of retrieved bit patterns.

15. A method as claimed in Claim 14 wherein the biometrics data sources are of different types.

Sub A5

16. A method as claimed in any one of the preceding Claims wherein a plurality of keys corresponding to a plurality of persons are generated and the corresponding bit patterns are stored in two or more parallel associative memories.

17. A method as claimed in any one of the preceding Claims wherein step (1) is performed a plurality of times to provide a plurality of samples and only invariant feature measures persistent in all samples are used to generate the key.

WO 00/14716

PCT/SG98/00067

23

18. A method of generating a representation of a biometrics image comprising the steps of:

- (1) capturing the biometric image;
- (2) normalizing the captured biometrics data,
- (3) extracting invariant features from the normalized data and representing the features as a bit pattern.

19. A method as claimed in Claim 18 wherein the features are selected from normalized data corresponding to a portion of the image.

20. A method as claimed Claim 18 or Claim 19 wherein the bit pattern is generated from the features using a representation scheme.

21. A method as claimed in Claim 20 wherein the features are represented according to importance.

22. A method of controlling access by generation of an access key from a person's biometrics data comprising the steps of:

- (1) capturing the person's biometrics data;
- (2) normalizing the captured biometrics data,
- (3) extracting invariant features from the normalized data and representing the features as an initial bit pattern;
- (4) storing the initial bit pattern in associative memory for retrieval;

~~SECRET~~ **SECRET**

WO 00/14716

PCT/SG98/00067

24

- (5) repeating steps (1)-(3) at a subsequent time to generate a subsequent bit pattern;
- (6) inputting the subsequent bit pattern to the associative memory to recall the stored bit pattern; and
- (7) generating the key from the recalled bit pattern.

23. A method of generating a key from the person's biometrics data which comprises the steps of:

- (1) capturing the person's biometric data;
- (2) normalizing the captured biometrics data,
- (3) extracting invariant features from the normalized data and representing the features as a bit pattern;
- (4) storing the bit pattern in associative memory for retrieval; and
- (5) generating the key from the retrieved bit pattern.

24. Apparatus for performing the method of any one of Claims 1-23.

25. Apparatus as claimed in claim 24 being a digital processor programmed to perform the method.

26. Apparatus as claimed in claim 24 or claim 25 including a biometrics capturing device.

27. Apparatus as claimed in claim 26 wherein the device captures live biometrics data.

WO 00/14716

PCT/SG98/00067

25

28. A codebook to store data from which, upon retrieval, a key is generated, the codebook comprising distributed associative memory.

09763624.061501